

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006年5月18日 (18.05.2006)

PCT

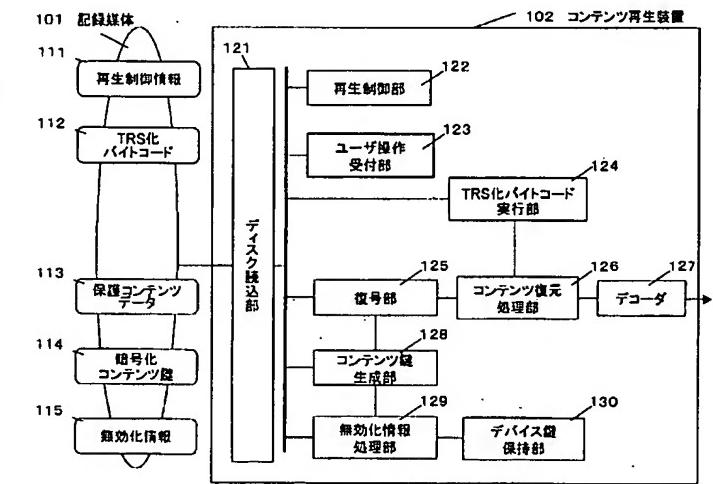
(10) 国際公開番号
WO 2006/051791 A1

- (51) 国際特許分類:
G06F 21/24 (2006.01) *GIIB 20/10 (2006.01)*
G09C 1/00 (2006.01) *GIIB 27/00 (2006.01)*
GIOL 19/00 (2006.01)
- (21) 国際出願番号: PCT/JP2005/020470
- (22) 国際出願日: 2005年11月8日 (08.11.2005)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
 特願 2004-326512
 2004年11月10日 (10.11.2004) JP
- (71) 出願人(米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真1006番地 Osaka (JP).
- (72) 発明者; および
 (75) 発明者/出願人(米国についてのみ): 小野田 仙一 (ON-ODA, Senichi). 山本 雅哉 (YAMAMOTO, Masaya). 村瀬 薫 (MURASE, Kaoru). 宮崎 雅也 (MIYAZAKI, Masaya).
- (74) 代理人: 中島 司朗, 外 (NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目2番1号淀川5番館 6F Osaka (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(締葉有)

(54) Title: DATA REPRODUCING METHOD AND DATA PROCESSING DEVICE

(54) 発明の名称: データ再生方法及びデータ処理装置



- 101... RECORDING MEDIUM
- 111... REPRODUCTION CONTROL INFORMATION
- 112... BYTCODE-FOR-TRS
- 113... PROTECTED CONTENT DATA
- 114... CONTENT KEY FOR ENCRYPTION
- 115... NULLIFICATION INFORMATION
- 121... DISK READING SECTION
- 122... CONTENT REPRODUCER
- 123... USER OPERATION RECEIVING SECTION
- 124... BYTCODE-FOR-TRS EXECUTING SECTION
- 125... DECODING SECTION
- 126... CONTENT RESTORING SECTION
- 127... DECODER
- 128... CONTENT KEY CREATING SECTION
- 129... NULLIFICATION INFORMATION PROCESSING SECTION
- 130... DEVICE KEY HOLDING SECTION

(57) Abstract: A recording medium, a data protective method, a data processing method, and a data processing device for protecting the contents so that even if a method for breaking the content protection is found out in consequence of a some accident or incident, the other content cannot be falsely used by the same way. Content data is protected by subjecting it to an altering processing such as XOR operation with a specific value in addition to encryption using a content key, and the bytecode for restoring the data from the altered data is protected by a method different from the content key.

(57) 要約: 何らかの事故や事件により、一旦コンテンツ保護を破る方法が発見されたとしても、他のコンテンツに対し、同じ方法でコンテンツを不正に利用することができないようにコンテンツを保護する記録媒体、データ保護方法、データ処理方法、及びデータ処理装置を提供する。コンテンツデータをコンテンツ鍵による暗号化だけでなく、特定の値とXOR演算する等の変形処理を施して保護し、変形データからの復元するためのバイトコードをコンテンツ鍵とは別の方で保護する。

WO 2006/051791 A1

ATTACHMENT A

WO 2006/051791 A1

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ヨーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

- 国際調査報告書